

PATENT
81940.0054

Express Mail Label No. EV 325 216 828 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Hiromi UKAI et al.

Serial No: Not assigned

Filed: July 15, 2003

For: METHOD AND APPARATUS FOR USING
CONTENTS

Art Unit: Not assigned

Examiner: Not assigned

TRANSMITTAL OF PRIORITY DOCUMENT

Mail Stop PATENT APPLICATION

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2002-321962 which was filed November 6, 2002, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

By: 

Anthony J. Orler

Registration No. 41,232

Attorney for Applicant(s)

Date: July 15, 2003

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2002年11月 6日

出願番号

Application Number:

特願2002-321962

[ST.10/C]:

[JP2002-321962]

出願人

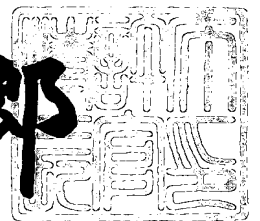
Applicant(s):

株式会社日立製作所

2003年 4月11日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3025191

【書類名】 特許願
【整理番号】 K02006801A
【あて先】 特許庁長官殿
【国際特許分類】 G06F 17/60
【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日
立製作所システム開発研究所内

【氏名】 鶴飼 ひろみ

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日
立製作所システム開発研究所内

【氏名】 平澤 茂樹

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日
立製作所システム開発研究所内

【氏名】 安細 康介

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日
立製作所システム開発研究所内

【氏名】 越前 功

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日
立製作所システム開発研究所内

【氏名】 吉浦 裕

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日
立製作所システム開発研究所内

【氏名】 岡山 祐孝

【発明者】

【住所又は居所】 東京都千代田区神田駿河台四丁目 6 番地 株式会社日立
製作所デジタルメディアグループ内

【氏名】 田胡 修一

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ保護システム

【特許請求の範囲】

【請求項 1】

プロバイダを識別するための第 1 のプロバイダ ID がコンテンツ保証機関によって埋め込まれたデジタルコンテンツを保持すると共にプロバイダを識別するための第 2 のプロバイダ ID が認証局によって埋め込まれた証明書を保持するプロバイダ装置から、前記デジタルコンテンツの提供を受けるコンテンツ利用端末において、

前記デジタルコンテンツと前記証明書を、前記プロバイダ装置から受信する受信処理部と、

前記証明書を用いて前記プロバイダが前記認証局によって許可されているか否かをチェックする第 1 のチェック処理部と、

前記証明書から前記第 2 のプロバイダ ID を読み出し、読み出された前記第 2 のプロバイダ ID と受信された前記デジタルコンテンツとを互いに対応付けて記録媒体へ記録する記録処理部と、

前記デジタルコンテンツから前記第 1 のプロバイダ ID を検出する検出処理部と、

前記記憶媒体から前記第 1 のプロバイダ ID を読み出し、前記第 1 のプロバイダ ID と前記第 2 のプロバイダ ID とを比較し、両プロバイダ ID が一致するか否かを判断する第 2 のチェック処理部と、

前記デジタルコンテンツを利用する利用処理部を備えたコンテンツ利用端末。

【請求項 2】

請求項 1 に記載のコンテンツ利用端末において、

前記利用処理部は、前記チェック処理部が前記両プロバイダ ID が一致しないと判断した場合に、前記デジタルコンテンツの利用を制限するコンテンツ利用端末。

【請求項 3】

請求項 1 に記載のコンテンツ利用端末において、

前記第 1 のプロバイダ I D は、前記コンテンツ保証機関によって、電子透かしにより前記デジタルコンテンツに埋め込まれているコンテンツ利用端末。

【請求項 4】

請求項 1 に記載のコンテンツ利用端末において、

前記両プロバイダ I D が一致しないと判断した場合に、前記認証局と前記コンテンツ保証機関と前記コンテンツ・ホルダーの少なくとも 1 つへ通知する通知処理部を備えたコンテンツ利用端末。

【請求項 5】

請求項 4 に記載のコンテンツ利用端末において、

前記通利処理部は、前記両プロバイダ I D が一致しないと判断した場合に、前記認証局と前記コンテンツ保証機関と前記コンテンツ・ホルダーの少なくとも 1 つへ、前記第 1 のプロバイダ I D と前記第 2 のプロバイダ I D の少なくとも 1 つを通知するコンテンツ利用端末。

【請求項 6】

請求項 1 に記載のコンテンツ利用端末において、

前記検出処理部は、前記デジタルコンテンツから前記第 1 のプロバイダ I D を検出できない場合に、前記デジタルコンテンツの流通経路が管理対象外であると判断し、

前記チェック処理部は、前記両プロバイダ I D が一致しないと判断した場合に、前記デジタルコンテンツの流通経路が不正であると判断するコンテンツ利用端末。

【請求項 7】

請求項 1 に記載のコンテンツ利用端末において、

前記記録媒体は、前記デジタルコンテンツを格納するためのコンテンツ蓄積部と、前記コンテンツ蓄積部に比較して耐タンパ性が高くかつ前記第 2 のプロバイダ I D を格納するためのライセンス管理部とを有するコンテンツ利用端末。

【請求項 8】

請求項 1 に記載のコンテンツ利用端末において、

前記デジタルコンテンツは、前記コンテンツ・ホルダを識別するためのコンテ

ンツ I D を、前記コンテンツ保証機関又は前記コンテンツ・ホルダによって埋め込まれ、

前記検出処理部は、前記デジタルコンテンツから前記第 1 のプロバイダ I D を検出できない場合に、前記デジタルコンテンツの流通経路が管理対象外であると判断し、さらに、前記デジタルコンテンツの流通経路が管理対象外であると判断した場合に、受信された前記デジタルコンテンツから前記コンテンツ I D を検出し、

前記利用処理部は、前記デジタルコンテンツに前記コンテンツ I D が埋め込まれていないと判断した場合に、前記デジタルコンテンツの利用を許可するコンテンツ利用端末。

【請求項 9】

請求項 1 に記載のコンテンツ利用端末において、

前記デジタルコンテンツは、当該コンテンツ利用端末を識別するための第 1 のユーザ I D を、前記プロバイダ装置によって埋め込まれ、

前記記録媒体は、当該コンテンツ利用端末を識別するための第 2 のユーザ I D を記憶し、

前記検出処理部は、前記第 2 のチェック処理部が前記両プロバイダ I D が一致すると判断した場合に、前記デジタルコンテンツから前記第 1 のユーザ I D を検出する検出し、

前記第 2 のチェック処理部は、前記記憶媒体から前記第 2 のユーザ I D を読み出し、前記第 1 のユーザ I D と前記第 2 のユーザ I D とを比較し、両ユーザ I D が一致するか否かを判断するコンテンツ利用端末。

【請求項 10】

デジタルコンテンツを端末へ提供するプロバイダ装置において、

プロバイダを識別するための第 1 のプロバイダ I D がコンテンツ保証機関によって埋め込まれたデジタルコンテンツを記憶すると共にプロバイダを識別するための第 2 のプロバイダ I D が認証局によって埋め込まれた証明書を記憶する記憶装置と、

前記端末からの要求に应答して、前記証明書を前記端末へ送信する第 1 の送信

処理部と、

前記端末が前記証明書を用いて前記プロバイダが前記認証局によって許可されているか否かをチェックすると共に前記証明書から前記第 2 のプロバイダ I D を読み出し、読み出された前記第 2 のプロバイダ I D と受信された前記デジタルコンテンツとを互いに対応付けて記録媒体へ記録した場合に、前記端末からの要求に応答して、前記デジタルコンテンツを前記端末へ送信する第 2 の送信処理部とを備え、

前記端末は、受信された前記デジタルコンテンツから前記第 1 のプロバイダ I D を検出し、前記記憶媒体から前記第 1 のプロバイダ I D を読み出し、前記第 1 のプロバイダ I D と前記第 2 のプロバイダ I D とを比較し、両プロバイダ I D が一致するか否かを判断するプロバイダ装置。

【請求項 1 1】

当該コンテンツ利用端末を識別するための第 1 のユーザ I D をデジタルコンテンツに埋め込むプロバイダ装置から、前記デジタルコンテンツの提供を受けるコンテンツ利用端末において、

当該コンテンツ利用端末を識別するための第 2 のユーザ I D を記憶する記憶装置と、

前記デジタルコンテンツを、前記プロバイダ装置から受信する受信処理部と、
受信された前記デジタルコンテンツを前記記録装置へ記録する記録処理部と、
前記デジタルコンテンツから前記第 1 のユーザ I D を検出する検出処理部と、
前記記憶部から前記第 2 のユーザ I D を読み出し、前記第 1 のユーザ I D と前記第 2 のユーザ I D とを比較し、両プロバイダ I D が一致するか否かを判断するチェック処理部とを備えたコンテンツ利用端末。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、デジタルコンテンツの流通経路を管理するためのシステム及び方法に関する。

【0 0 0 2】

【従来の技術】

【特許文献 1】特開2000-330873号公報

【特許文献 2】特開2001-256192号公報

近年、ストリーミング技術やデータ圧縮技術が進歩すると共に、ブロードバンド通信が急速に家庭に普及し始めたことから、動画や音楽などの大容量のデジタルコンテンツが流通し始めている。デジタルコンテンツはコピーや加工が容易にでき、しかも、品質劣化が生じないという利点がある一方で、不正な利用によって著作権が侵害されるという問題も大きい。

【0003】

この問題に対して、デジタルコンテンツを暗号化して鍵をかけ、その鍵を別途ライセンスとして利用者／利用端末に配布することで著作権を保護する方式がある。コンテンツの利用時には、システムがライセンスの有無やライセンスに含まれている利用条件情報を参照し、利用期限などの利用条件を満たしている場合のみ、コンテンツが利用できる仕組みになっている。この方式によれば、コンテンツが不正にコピーされても、ライセンスを持たない利用者はコンテンツを利用することはできない。更に、鍵の生成過程に端末固有の番号を組み込むなどして利用端末毎に異なる鍵を生成して配布し、コンテンツと共にライセンスを他の端末にコピーしても、コピー先の端末では鍵が利用できないようにすることによって、コンテンツの不正利用を防ぐ方式もある。

【0004】

また、電子透かし (Digital watermark) を用いてデジタルコンテンツに著作権情報を埋めこみ、不正利用を検出する技術も提案されている。例えば、特許文献 1 には、ウェブページなどで利用されるコンテンツに電子透かしで識別情報を埋めこんでおき、利用許可 DB に識別情報と利用条件を登録しておき、監視センターがコンテンツに埋めこまれた識別情報と利用許可 DB の識別情報とを照合して不正利用を検出する技術が開示されている。また、特許文献 2 には、購入対象コンテンツを特定する情報とコンテンツ配信者と購入者ごとに割り振られた ID 番号を、透かし情報として、流通するコンテンツデータに埋め込むことが開示されている。

【 0 0 0 5 】

【発明が解決しようとする課題】

上記のライセンスを用いた従来技術では、ライセンス情報が改ざんされたり、暗号が解かれたコンテンツが不正に流通する可能性があった。また、コンテンツが流出した場合は、どこから流出したのかを特定する手段がなく、流出を止めることが難しかった。

【 0 0 0 6 】

上記の電子透かしを用いて不正利用を監視する従来技術では、ウェブページへの不正な掲載を監視することは可能であるが、ユーザ端末間でコンテンツをコピーするなど、監視センターからアクセスできない場所での不正利用を監視することはできなかった。また、現在、ウェブページ上では膨大な数のコンテンツが利用されているが、その全てを監視することは困難である。

【 0 0 0 7 】

本発明の目的は、コンテンツ・ホルダとコンテンツ利用者の片方又は双方に対しデジタルコンテンツの流通経路を保証するシステム及び方法を提供することである。

【 0 0 0 8 】

本発明の目的は、デジタルコンテンツの不正流通を抑制するシステム及び方法を提供することを提供することである。

【 0 0 0 9 】

【課題を解決するための手段】

本発明は、コンテンツおよびコンテンツのプロバイダの身元を保証するための認証局を設け、認証局からコンテンツを配信する許可を受けたプロバイダにのみ、認証局が証明書を発行する。証明書にはプロバイダを一意に識別するための識別子（プロバイダID）が記されている。プロバイダIDは認証局が管理して発行する。コンテンツ・ホルダは認証局によって身元が保証されているプロバイダ、すなわち、認証局発行の証明書を所有するプロバイダにコンテンツの配信を依頼する。プロバイダを許可制にすることにより、コンテンツの流通経路を特定することが可能となる。

【 0 0 1 0 】

コンテンツ・ホルダからコンテンツプロバイダへのコンテンツの仲介は、認証局が認定したコンテンツ保証機関が行なう。コンテンツ保証機関は、コンテンツをコンテンツ・ホルダから受け取り、プロバイダのプロバイダIDを電子透かしを用いて埋めこみ、埋めこんだIDに対応するコンテンツプロバイダに渡す。一度書きこまれたプロバイダIDは書き換えできないようにする。これにより、プロバイダが流通経路を改ざんできなくなる。

【 0 0 1 1 】

プロバイダはコンテンツを端末に配信するが、そのコンテンツはコンテンツ保証機関を仲介してコンテンツ・ホルダから受け取ったコンテンツであり、自分自身を示すプロバイダIDが透かしで挿入されている。また、プロバイダは認証局から発行された証明書を所有しており、その証明書には自分自身を示すプロバイダIDが記載されている。

【 0 0 1 2 】

利用者端末では、プロバイダが所有する証明書を参照し、プロバイダが認証局によって保証されていることを確認してからコンテンツを受信する。受信したコンテンツはコンテンツ蓄積部に記憶されるが、このとき、コンテンツを端末内で一意に識別するためのコンテンツ名とプロバイダを識別するためのプロバイダIDとを耐タンパ領域に記憶する。耐タンパ領域とは、外部からの不正なアクセスに備えるための物理的・論理的構造を備えた領域である。端末には透かし検出機能を設け、コンテンツの利用時には、コンテンツ保証機関によってコンテンツに埋め込まれたプロバイダIDの透かしを検出し、利用者による書き換えが不能な領域に記憶されたプロバイダのプロバイダIDと透かしのプロバイダIDとが一致しているかどうかを確認する。一致している場合には、コンテンツの流通経路は正規であると判断してコンテンツを利用できるようにし、一致しない場合にはコンテンツの流通経路は不正であると判断してコンテンツの利用を中断してコンテンツ保証機関に通知する。これにより、不正な経路で流通しているコンテンツとそのプロバイダを検出できるようになる。また、ネットポリスを設けることなく、端末で不正が検出できるようになる。

【 0 0 1 3 】

【発明の実施の形態】

図 1 は、本発明の一実施例の全体の構成を示した図である。本発明の実施の形態のコンテンツ保護システムは、デジタルコンテンツ（以下、単に「コンテンツ」という）およびプロバイダ 4 0 の身元を保証する認証局 1 0 と、コンテンツ（又はコンテンツの著作権等）を所有するコンテンツ・ホルダ 2 0 と、コンテンツを仲介するコンテンツ保証機関 3 0 と、コンテンツを利用者の端末 5 0 へ提供（配信）するプロバイダ 4 0 と、利用者がコンテンツを利用するための端末 5 0 とを有する。コンテンツ保証機関 3 0 とプロバイダ 4 0 は、認証局 1 0 の許可が必要である。認証局 1 0 とプロバイダ 4 0 の間、認証局 1 0 とコンテンツ保証機関 3 0 の間、コンテンツ・ホルダ 2 0 とコンテンツ保証機関 3 0 の間、コンテンツ保証機関 3 0 とプロバイダ 4 0 の間、プロバイダ 4 0 と端末 5 0 の間は夫々、ネットワークを介して接続可能であるのが好ましい。但し、認証局 1 0 とプロバイダ 4 0 の間、認証局 1 0 とコンテンツ保証機関 3 0 の間は、ネットワークを介して接続されなくてもよい。認証局 1 0、コンテンツ・ホルダ 2 0、コンテンツ保証機関 3 0、プロバイダ 4 0、端末 5 0 は夫々、処理装置（CPU）、記憶装置、通信装置を備えるのが好ましい。さらに、端末 5 0 は、入力装置、出力装置（表示装置、スピーカを含む）を備えるのが好ましい。プロバイダ 4 0 は、サーバ装置であるのが好ましい。処理装置が、プログラムに従って処理を実行することによって、各装置の機能が実現される。

以下、コンテンツにプロバイダ ID を透かしで挿入する場合について説明する。

【 0 0 1 4 】

コンテンツ・ホルダ 2 0 が所有するコンテンツ 1 0 1 がプロバイダ 4 0 から端末 5 0 に配信されて利用される場合を例に説明する。

【 0 0 1 5 】

まず、コンテンツ 1 0 1 をコンテンツ・ホルダ 2 0 からコンテンツ保証機関 3 0 に送る。コンテンツ保証機関 3 0 は、プロバイダ 4 0 のプロバイダ ID を透かし挿入機能 3 1 を用いて埋め込む。プロバイダ ID とは、プロバイダを一意に識別するための識別子である。ここで、プロバイダ 4 0 のプロバイダ ID を P 1 と

する。透かしの改ざんを防ぐために、一度書きこまれた透かしは書き換え不可能な仕組みを設けるようにする。コンテンツ 1 0 1 はプロバイダ I D を埋め込まれてコンテンツ 1 0 2 となる。コンテンツ保証機関 3 0 が、コンテンツ 1 0 2 をプロバイダ 4 0 に送信し、プロバイダ 4 0 が、コンテンツ 1 0 2 をコンテンツ D B 4 5 に登録する。プロバイダ 4 0 にコンテンツを渡す前に書き換えできないプロバイダ I D を埋め込むことにより、プロバイダ 4 0 がプロバイダ I D を改ざんして配信する不正を防ぐことができる。コンテンツ保証機関 3 0 がコンテンツの仲介を行うのではなく、透かしの埋め込みだけを行い、コンテンツ・ホルダ 2 0 からプロバイダに直接コンテンツを流しても構わない。透かしの埋め込みについては、特開 2001-256192 号公報等に記載されている。

【 0 0 1 6 】

プロバイダ 4 0 はプロバイダ証明書 4 1 を所有する。プロバイダ証明書 4 1 は認証局 1 0 が発行する証明書であり、この証明書を所有するプロバイダは本実施例の方式でコンテンツを配信できるプロバイダである。ただし、プロバイダが不正なコンテンツを流すなどした場合には証明書は無効となる。無効な証明書のリストが C R L (Certificate Revocation List) 4 4 である。認証局 1 0 が C R L 4 4 を作成して、コンテンツ保証機関 3 0 へ配布し、さらに、コンテンツ保証機関 3 0 が C R L 4 4 をプロバイダ 4 0 へ配布する。また、認証局 1 0 が C R L 4 4 を端末 5 0 へ配布する。また、証明書に有効期限（例えば、1 週間、1 か月等）を設け、頻繁に新規の証明書を発行するようにし、期限の切れた証明書は無効とみなすことによって、C R L を用いずにプロバイダ証明書の有効性を保持する方法も考えられる。

【 0 0 1 7 】

端末 5 0 は、利用者からコンテンツ受信要求を受け、その要求の応答して、プロバイダ 4 0 にコンテンツ 1 0 2 の配信を要求する場合、まず、端末 5 0 はプロバイダチェック機能 6 2 を使ってプロバイダの正当性をチェックする。

【 0 0 1 8 】

図 2 は、プロバイダチェック機能 6 2 の処理の流れを示した図である。プロバイダ認証機能 5 1 は、プロバイダ証明書 4 1 を参照してプロバイダ認証を行う。

端末 5 0 は、コンテンツの配信要求に先立って、プロバイダ証明書 4 1 を、プロバイダ 4 0 に要求する。端末 5 0 は、そのプロバイダ証明書 4 1 の要求に対して、プロバイダ証明書 4 1 をプロバイダ 4 0 から受信した場合に、プロバイダ 4 0 がプロバイダ証明書を所有しており、プロバイダ認証が成功すると判定し、一方、プロバイダ証明書 4 1 をプロバイダ 4 0 から受信できない場合に、プロバイダ 4 0 がプロバイダ証明書 4 1 を所有しておらず、プロバイダ認証が失敗したと判定する (2 1 1)。プロバイダ認証が失敗した場合は無認可プロバイダであると判断し (2 1 2)、プロバイダ認証を終了する (2 4 1)。プロバイダ認証が成功した場合は、C R L 4 4 にプロバイダ証明書 4 1 の証明書番号が記載されていないかを確認し (2 2 1)、書かれていなければ認可プロバイダであると判断する (2 2 2)。C R L 4 4 にプロバイダ証明書 4 1 の証明書番号が記載されている場合は無認可プロバイダであると判断し (2 3 1)、プロバイダチェックの処理を終了する (2 4 1)。

【 0 0 1 9 】

一方、プロバイダ 4 0 は端末 5 0 が本方式によるコンテンツ保護機能に対応しているか否かを端末認証機能 4 2 を用いて判断し、対応している場合には配信機能 4 3 を用いてコンテンツ 1 0 2 を端末 5 0 へ配信する。一方、対応していない場合には配信を中断又は中止する。端末 5 0 が本方式によるコンテンツ保護機能に対応しているか否かは端末が固有に所有する端末 I D 5 2 をチェックするなどして判断する。つまり、プロバイダ 4 0 が、本方式によるコンテンツ保護機能に対応している端末 I D を記憶しておき、コンテンツを配信する際に、端末 5 0 から受信した端末 I D 5 2 と予めプロバイダ 4 0 に記憶する端末 I D を比較し、両者の端末 I D が一致した場合に、対応端末と判断し、両者 I D が一致しない場合に、対応端末でないと判断する。対応端末にのみコンテンツを配信することにより、コンテンツの流通経路をチェックする機能を持たない端末へのコンテンツ配信を防ぐことができる。ただし、端末認証機能 4 2 は必須機能ではない。端末認証機能 4 2 がない場合は本方式のコンテンツ保護機能に対応していない端末にコンテンツが配信されて利用されるであろうし、そのコンテンツが他の端末にコピーされて利用される可能性も高い。コンテンツが端末間でコピーされたとしても

、大量にコピーされなければ被害は少ないが、悪質なプロバイダによって大量に配信されたり、利用者間で大量にコピーされたりして被害が拡大するおそれもある。このような場合であっても、本方式のライセンスチェック機能を設けた端末が市場に出回っていれば、その端末で不正コンテンツを検出できるため、被害が広がる前に不正に出回っているコンテンツをたやすく見つけることができる。従って、端末認証機能 4 2 は必須機能ではないが、端末認証機能 4 2 を設けることによってコンテンツの流出防止レベルを高くすることができる。

【 0 0 2 0 】

図 3 は端末 5 0 におけるコンテンツ受信の流れを示している。プロバイダチェック機能 6 2 でプロバイダが認可されているか否かを判断した後、認可プロバイダである場合には (3 1 1) 、受信機能 5 3 を用いてコンテンツを受信する (5 3) 。受信されたコンテンツに名前を付けてコンテンツ記憶部 5 4 に保存する (3 2 1) 。また、プロバイダ証明書 4 1 からプロバイダ ID p 1 を読み出し、コンテンツ名と組にしてライセンス管理部 5 5 に記憶する (3 3 1) 。ライセンス管理部 5 5 は、コンテンツ蓄積部 (例えば、ハードディスクやフラッシュメモリ等) に比較して、耐タンパ性が高い領域 (耐タンパ構造を持つ領域、例えば、IC カードチップ等) である。プロバイダ ID は、プロバイダ証明書に記載されている。ここではプロバイダ 4 0 のプロバイダ証明書 4 1 には、プロバイダ ID とし て p 1 が記載されているものとし、コンテンツ名 n 1 と配信元プロバイダ ID p 1 を 5 6 としてライセンス管理部 5 5 に記憶する。

【 0 0 2 1 】

無認可プロバイダの場合は受信機能 5 3 を用いてコンテンツを受信する (5 3) 。コンテンツに名前を付けてコンテンツ記憶部 5 4 に保存する (3 2 1) 、コンテンツ受信の処理を終了する (3 4 1) 。ライセンス管理部 5 5 にコンテンツ名と配信元プロバイダ ID の組 5 6 を記憶するのは、以下の理由による。コンテンツに埋めこまれたプロバイダ ID はコンテンツを配信するはずのプロバイダの識別子であり、実際の配信元プロバイダの識別子はプロバイダ証明書に記載されたプロバイダ ID である。プロバイダ ID は認証局が管理し発行しているため、正規の流通経路で配信されたコンテンツであれば両者は同じ ID となる。従って

、コンテンツに埋めこまれたプロバイダIDと配信元プロバイダIDを比較することにより、コンテンツの流通経路の正当性を判断することが可能となる。この判断がいつでもできるようにするために、コンテンツ名と配信元プロバイダIDの組56をライセンス管理部55に記憶する。この情報56はコンテンツの流通経路の正当性を保証するための一種のライセンスと考えることができ、ライセンスを端末側で自動的に生成することが可能となる。ライセンス管理部55は不正アクセスや改ざんを防止するための耐タンパ構造となっているため、コンテンツ名と配信元プロバイダIDの組56をユーザが改ざんすることはできない。耐タンパ構造とは、外部からの不正なアクセスに備えるための物理的・論理的技術を組み込んだ構造をさし、既にICカードなどの分野で実用になっている。尚、一般的に、下流側装置（クライアント装置）がコンテンツを受信する場合に、下流側装置から上流側装置（サーバ装置）へ下流側装置の証明書を送信し、上流側装置がその証明書を用いて下流側装置を認証する。しかし、本発明では、下流側装置がコンテンツを受信する場合に、上流側装置から下流側装置へ上流側装置の証明書を送信し、下流側装置がその証明書を用いて上流側装置を認証することに特徴がある。

【0022】

ここまでコンテンツ・ホルダ20、コンテンツ保証機関30、プロバイダ40を別々の機関として説明したが、全部、あるいは、一部を一つの機関が兼ねてもよい。

【0023】

次に、端末でのコンテンツ利用時の流れを説明する。まず、ライセンスチェック機能59によってコンテンツの流通経路の正当性を判断し、次に、流通経路が不正でなければコンテンツ利用機能60によって音楽の再生や映像の再生などを行ない、流通経路が不正であれば不正通知機能61によって認証局10その他の機関へ通知する。

【0024】

図4はプロバイダIDを使用したライセンスチェック400の流れを示した図である。ライセンスチェックにはプロバイダID以外にコンテンツIDやユーザ

I Dを使用する方法も考えられるため、図1ではそれらを総称してライセンスチェック機能59と表している。プロバイダI Dを使用したライセンスチェック400では、まず、透かし検出機能58によってコンテンツに埋めこまれた透かしの検出を行い、次に、プロバイダI Dが検出されたか否かを判断する(411)。プロバイダI Dが検出されない場合は「コンテンツの流通経路は管理対象外」と判断して処理を終了する(481)。

【0025】

プロバイダI Dが検出された場合は、透かしで検出されたプロバイダI DをP1の値とし、再生するコンテンツのコンテンツ名をコンテンツ蓄積部54から読み出し(431)、該当するコンテンツ名がライセンス管理部55に記憶されているか否かを判断する(441)。コンテンツ名が記憶されていない場合はライセンス管理部55にライセンス情報56が存在しないため、コンテンツが端末間で不正にコピーされたか、あるいは不正プロバイダが正規のプロバイダのコンテンツを流通させたかの可能性が考えられるため「コンテンツの流通経路は不正」と判断して処理を終了する(481)。

【0026】

処理441においてコンテンツ名が記憶されていると判断された場合は、ライセンス情報56の配信元プロバイダI Dの値をp1とし、P1とp1の値を比較する(461)。P1とp1の値が等しい場合は「コンテンツの流通経路は正規である」と判断し(471)、P1とp1の値が不等な場合は正規の流通経路ではないため「コンテンツの流通経路は不正である」とあると判断して(462)処理を終了する(481)。透かし検出機能58及びライセンスチェック機能59は、コンテンツの利用時に動作してもよいし、プロバイダ40からコンテンツの受信及びコンテンツ蓄積部103への記録時に動作してもよい。

【0027】

図7を用いて、プロバイダI Dを使用したコンテンツ利用の流れを説明する。図7にはユーザI DとプロバイダI DとコンテンツI Dを使用したコンテンツ利用の流れを示しているが、ここではプロバイダI Dのみを使用するので、ユーザI Dを使用したライセンスチェック600、および、コンテンツI Dの検出50

0に関連する処理は行なわない。まず、利用者からコンテンツ利用要求と受け、その要求に応答して、プロバイダIDを使用したライセンスチェック400を行ない、その結果が「コンテンツの流通経路は正規」であった場合(711)はステップ600、721、722、61の処理は省略し、コンテンツ利用機能60によってコンテンツを利用する。「コンテンツの流通経路は不正」であった場合(721)はエラーである旨を表示し(722)、不正通知機能61によって認証局10に通知し、コンテンツの利用は中止して処理を終了する(741)。「コンテンツの流通経路は管理外」であった場合(731)はステップ500、732、722、61、および、600、721、722の処理を省略してコンテンツ利用機能60によってコンテンツを利用して処理を終了する(741)。

図8は、プロバイダIDを使用したコンテンツの流通経路管理と端末での利用の可否を示した図である。端末にて不正を検出したときにはコンテンツの利用を中止するだけでもよく、不正通知機能61はなくてもよし、コンテンツ蓄積部54からコンテンツを削除してもよい。また、端末50は、コンテンツ・ホルダ20やコンテンツ保証機関30へ不正通知を行ってもよい。

【0028】

コンテンツを配信するプロバイダのIDを透かしでコンテンツに埋めこみ、一度埋めこまれた透かしは書き換えできないようにすることによって、コンテンツの配信者を特定するための情報をコンテンツと共に流通させることが可能となる。コンテンツの利用時にはコンテンツを実際に配信したプロバイダのIDと透かしに埋めこまれたプロバイダIDとを比較し、不正な流通経路の場合はコンテンツの利用を中止する機能を設けることによって、コンテンツの不正な利用を防止することが可能となる。さらに、不正な流通が端末で検出された場合にコンテンツ保証機関に不正を通知する機能を設けることにより、不正を取り締まるためのネットポリスを設けることなく、端末で不正が検出できるようになる。また、不正通知機能を設けなくても不正なプロバイダから配信されたコンテンツは端末で利用できないため、不正プロバイダの信用がなくなることが予想され、十分な不正抑止効果が期待できる。

【0029】

近年ではコンテンツにメタデータと呼ばれるコンテンツの属性をコンテンツのヘッダ部などに付随している場合が多く、メタデータとしてコンテンツIDが付随している場合もある。図1ではライセンス管理部55にコンテンツ名と配信元プロバイダの組で構成されるライセンス情報56を記憶するようにしたが、メタデータにコンテンツIDが付随している場合は、コンテンツ名と配信元プロバイダIDの組の代わりにコンテンツIDと配信元プロバイダIDの組をライセンス情報602としてライセンス記憶部55に記憶してもよい。ライセンス情報56にコンテンツIDを使用する場合は図4のステップ431および441においてコンテンツ名の代わりにコンテンツIDを使用する。また、メモリカードなどのポータブルなメディアにライセンス管理部55とコンテンツ蓄積部54を設けコンテンツを移動させて利用できるようにすることも考えられる。

【0030】

コンテンツ103、および、ライセンス56はファイルの形で存在する必要はない。例えば、ストリーミング技術によりコンテンツを受信しながら利用する場合はコンテンツの一部が端末の主記憶領域に存在する。従って、コンテンツ蓄積部54とライセンス管理部55は主記憶であっても構わない。ストリーミング技術に本方式を適用する場合は、コンテンツの利用と同時にプロバイダIDの透かし検出を行い、コンテンツ利用が不可と判断した時点でコンテンツの利用を中止するなどの処理を行う。

【0031】

次に、コンテンツにコンテンツIDとプロバイダIDを透かしで挿入する場合について説明する。

【0032】

プロバイダIDに加えてコンテンツIDを透かしで挿入する方法も考えられる。例えば、コンテンツ・ホルダ20が透かし挿入機能31によってコンテンツ101にコンテンツIDを挿入する。コンテンツIDは認証局が管理し、例えばIDの上位にはコンテンツ・ホルダごとに決められたIDを使用するなどして、どのコンテンツ・ホルダが所有するコンテンツかが分かるようなIDを付与する。認証局はコンテンツ・ホルダのIDのみを管理し、コンテンツ・ホルダ内でコン

テンツIDを付与しても良い。コンテンツIDの透かし挿入は、各コンテンツ・ホルダからコンテンツ保証機関30に依頼しても良いが、コンテンツIDにはそのコンテンツを所有するコンテンツ・ホルダを一意に識別するための識別子が組み込まれているため、プロバイダにコンテンツを渡す前にきちんとコンテンツ・ホルダがコンテンツIDを確認できることが不正な流通を防ぐためには必要であり、プロバイダにおいてコンテンツIDを挿入するのは危険である。

【0033】

図5にコンテンツIDの検出の流れ500を示す。透かし検出機能58によってコンテンツの透かしを検出し、コンテンツIDが検出された場合(521)は、「コンテンツIDあり」と判断し(522)、そうでなければ「コンテンツIDなし」と判断して(531)終了する(541)。

【0034】

図7を用いて、コンテンツIDとプロバイダIDを用いた場合のコンテンツ利用の流れを説明する。ここではユーザIDは使用しないので、ユーザIDに関する処理は省略する。プロバイダIDを使用した場合のコンテンツ利用の流れと同様にプロバイダIDを使用したライセンスチェック400の後、ステップ400の処理結果によって異なる処理を行なう。ステップ711、ステップ721の後にはプロバイダIDを使用した場合のコンテンツ利用の流れと同じ処理を行なう。ステップ731においてコンテンツの流通経路が管理外であると判断された場合には、コンテンツIDの検出500を行ない、コンテンツIDがあると判断された場合は(732)エラー表示を行ない(722)、不正通知機能61を用いてコンテンツ保証機関に不正内容を通知し、コンテンツの利用を中止して終了する(741)。不正通知機能61はなくてもよい。732においてコンテンツIDがないと判断された場合はコンテンツ利用機能60によってコンテンツを利用して終了する(741)。

【0035】

図9は、コンテンツIDとプロバイダIDを使用したコンテンツの流通経路管理と端末での利用の可否を示した図である。端末にて不正を検出したときには保証機関に通知せずに、コンテンツの利用を中止するだけでもよい。コンテンツI

Dの透かしがあり、コンテンツのプロバイダ流通経路が管理対象外である場合、ここではコンテンツの利用はできないようにしているが、運用によっては利用できるようにしても構わない。また、コンテンツIDの透かしが検出されず、コンテンツのプロバイダ流通経路が不正であると判断された場合、ここではコンテンツの利用はできないようにしているが、運用によっては、コンテンツIDの透かしが検出されない場合はコンテンツが利用できるようにしても構わない。運用の仕方は複数考えられるが、コンテンツ・ホルダに近い上流側でコンテンツの流通をきつく管理する場合はコンテンツIDの埋めこみを必須とした前提でコンテンツ利用の可否を判断するようにし、そうでない場合にはコンテンツIDの透かし検出はコンテンツ利用の可否に影響しないように運用すればよい。

【 0 0 3 6 】

このように、コンテンツにコンテンツIDとプロバイダIDを挿入することにより、コンテンツ・ホルダープロバイダ間の流通経路の確かさを確認することが可能となる。コンテンツIDにコンテンツ・ホルダを識別する仕組みを入れ、コンテンツにコンテンツIDを挿入してIDを書き換えできないようにすることにより、コンテンツがどのコンテンツ・ホルダからきたのかがわかるようになり、コンテンツの出所の確かさを確認できるようになる。すべてのコンテンツへのコンテンツIDの透かし挿入を前提とすると、コンテンツIDが挿入されていてプロバイダ流通経路が管理対象外である場合は不正コンテンツであり、コンテンツはコンテンツ・ホルダにてコンテンツIDを挿入された後、流出していたことが分かる。また、コンテンツ保証機関30を識別できる透かしを挿入するなどさまざまな流通過程で透かしを挿入していくことによって、どこから流出したのかを検出することも可能となる。

【 0 0 3 7 】

次に、コンテンツにユーザIDを透かしで挿入する場合について説明する。

【 0 0 3 8 】

コンテンツを利用する機器を指定するために、機器固有の番号を組み込んだIDをユーザIDとし、ユーザIDをコンテンツに透かしで埋め込む方法が考えられる。ユーザIDとして使用できるものに、端末固有の番号や端末でコンテンツ

を利用するために必要なソフトウェアの製品番号、ICカードのカード番号、メモリカードの製造番号などがあげられる。ユーザIDの透かし埋め込みは、プロバイダ40に透かし挿入機能31を設けて、コンテンツを配信する際にプロバイダ40が行なう方法と、端末50に透かし挿入機能31を設けて、コンテンツ受信後に端末50が行なう方法の二通りが考えられる。

【0039】

図6にユーザIDを使用したライセンスチェック600の流れを示す。処理が開始すると(601)、透かし検出機能58がコンテンツの透かしを検出し、その結果、ユーザIDが検出された場合は(611)、U1に検出されたユーザIDの値を代入し(621)、u1に端末の製造番号を代入する(631)。U1とu1の値が等しい場合は(641)「コンテンツの流通経路は正規である」と判断し(471)、層でない場合は「コンテンツの流通経路は不正である」と判断して(442)処理を終了する(651)。ステップ611においてユーザIDが検出されなかった場合は「コンテンツの流通経路は管理対象外である」と判断する(412)して処理を終了する(651)。ここでは、ユーザIDには端末の製造番号を使用しているが、端末を一意に識別することができさえすれば、ユーザIDは端末の製造番号と同じでなくてもよい。

【0040】

ユーザIDを用いた場合のコンテンツ利用の流れを図7を用いて説明する。ここではコンテンツIDとプロバイダIDは使用しないので、処理を開始(701)すると、コンテンツIDとプロバイダIDに関する処理は省略し、ステップ600にてユーザIDを使用したライセンスチェックを行ない、ステップ721にてコンテンツの流通経路は不正であると判断された場合はエラーを表示し(722)、コンテンツの利用を中止して処理を終了する(741)。ステップ721の判断が失敗した場合にはコンテンツ利用機能60によってコンテンツを利用して処理を終了する(741)。

【0041】

図10は、ユーザIDを使用したコンテンツの流通経路管理と端末での利用の可否を示した図である。ここでは、端末の製造番号をユーザIDに使用する場合

について示している。透かしのユーザIDと端末製造番号が異なる場合は、利用を許可された端末とは別の端末でコンテンツ利用しようとしていると判断してコンテンツの利用を中止する。コンテンツ利用の可否や保証機関へ通知するか否かなどの運用については、この図の通りである必要はない。

【0042】

このように、利用する端末を指定するための識別子をユーザIDとしてコンテンツに透かしで挿入し、利用端末においてユーザIDを検出して特定されるか否かによってコンテンツの利用を制限する機能を設けることにより、コンテンツを利用する端末を特定することが可能となる。また、利用者の端末から不正に流出したコンテンツには端末を識別するためのユーザIDが透かしで埋めこまれているため、透かしを検出することによって、どの端末からコンテンツが流出したかを確認することが可能となる。

【0043】

次に、コンテンツにプロバイダIDとユーザIDを透かしで挿入する場合を説明する。

【0044】

ユーザIDに加えてプロバイダIDを透かしで挿入する方法も考えられる。上述したプロバイダIDを挿入する場合とユーザIDを挿入する場合との組み合わせで実現できる。プロバイダIDとユーザIDを用いた場合のコンテンツ利用の流れを図7を用いて説明する。ここではコンテンツIDは使用しないので、コンテンツIDの検出とそれに関連する処理は省略する。処理を開始(701)してプロバイダIDを使用したライセンスチェック400を行い、ステップ711にて「コンテンツの流通経路は正規」と判断された場合、ユーザIDを使用したライセンスチェック600を行う。その結果、「コンテンツの流通経路は不正」と判断された場合(721)はエラーを表示し(722)、コンテンツ保証機関に通知(61)してコンテンツの利用は中止して処理を終了(741)する。ステップ721の判断が失敗した場合はコンテンツ利用機能60によりコンテンツを利用して処理を終了(741)する。ステップ721にて「コンテンツの流通経路は不正」と判断された場合は上述のプロバイダIDを用いた場合のコンテンツ

利用の流れと同様にステップ 7 2 2、6 1 の処理を行って終了 (7 4 1) する。ステップ 7 3 1 にて「コンテンツの流通経路は管理外」と判断された場合は、コンテンツ ID に関連するステップ 5 0 0、7 3 2、7 2 2、6 1 の一連の処理は省略し、ステップ 6 0 0 に進む。ステップ 6 0 0 にてユーザ ID を使用したライセンスチェックを行い、ステップ 7 2 1 にて「コンテンツの流通経路は不正」と判断された場合はエラーを表示 (7 2 2) して利用を中止し、そうでない場合はコンテンツ利用機能 6 0 によってコンテンツを利用して終了 (7 4 1) する。

【 0 0 4 5 】

図 1 1 は、プロバイダ ID とユーザ ID を使用したコンテンツの流通経路管理と端末での利用の可否の例を示した図である。端末での利用の可否と保証機関に通知するか否かなどについてはいろいろな運用の仕方が考えられる。例えば、プロバイダの流通経路は正規であるが端末流通経路は不正である場合、図 1 1 ではコンテンツの利用は不可であり、保証機関に通知するようにしている。このような流通経路の例として、正規に購入した個人が不正なプロバイダになり、大量に配布してしまうという可能性も考えられる。そのようなときでも、保証機関への通知機能により、正規に配信されている数と保証機関に不正が通知された数とを比較して、明らかに不正通知件数が多い場合はそのコンテンツは不正に流通している可能性が高いと判断することもできる。その他の運用方法としては、図 1 1 では利用不可の場合については、エラーだけを表示したり、正規のプロバイダからの購入を勧める表示をしたり、ライセンス購入用のサイトを別途設けてそのサイトに接続するなどが考えられる。

【 0 0 4 6 】

このように、プロバイダ ID とユーザ ID を透かしで挿入することでプロバイダ-端末間のコンテンツの正規の流通経路をコンテンツに埋めこんで流通させることができるようになり、コンテンツの実際の流通経路とコンテンツに埋めこまれた正規の流通経路を比較することにより、プロバイダの正当性と端末の正当性を確認できるようになる。

【 0 0 4 7 】

次に、コンテンツにコンテンツ ID とプロバイダ ID とユーザ ID を透かしで

挿入する場合を説明する。

【 0 0 4 8 】

コンテンツ ID、プロバイダ ID、ユーザ ID を透かしで挿入する方法も考えられる。コンテンツ ID とプロバイダ ID とユーザ ID を用いた場合のコンテンツ利用の流れを図 7 を用いて説明する。処理の開始 (7 0 1) からステップ 7 3 1 までは、上述のプロバイダ ID とユーザ ID を用いた場合と同様である。ステップ 7 3 1 にて「コンテンツの流通は管理外」と判断した場合、コンテンツ ID の検出 (5 0 0) を行ない、コンテンツ ID が検出された場合は (7 3 2) エラーを表示し (7 2 2)、コンテンツ保証機関に通知して (7 2 2)、処理を終了する (7 4 1)。コンテンツ ID が検出されなければ、プロバイダ ID とユーザ ID を用いた場合と同様にステップ 6 0 0、7 2 1、7 2 2、6 0 の処理を行なって終了する (7 4 1)。コンテンツ ID がすべてのコンテンツに挿入されていることを前提とするか否かによってコンテンツ利用の流れは変わる。無料のコンテンツや個人制作のコンテンツ (無料コンテンツ) にはコンテンツ ID が挿入されないことも想定し、ここでは、コンテンツ ID が挿入されていない場合でもコンテンツが利用できる流れになっている。また、コンテンツ ID が挿入されているコンテンツは必ず認可されたプロバイダ経由で配信されると想定し、コンテンツ ID が挿入されていてプロバイダ流通経路が管理対象外である場合は、不正な配信と考えてコンテンツの利用を中止する流れになっている。

【 0 0 4 9 】

図 1 2 に、コンテンツ ID、プロバイダ ID、ユーザ ID を使用したコンテンツの流通経路管理と端末での利用の可否の例を示す。コンテンツ ID が挿入されていないコンテンツは全て利用できない設定にしたり、各 ID を使ったライセンスチェックの結果が管理対象外の場合は、コンテンツの利用の流れは正規の流通経路の場合と同じとするなど、いろいろな運用が考えられる。

【 0 0 5 0 】

このように、コンテンツ ID とプロバイダ ID とユーザ ID を透かしで挿入することにより、コンテンツ・ホルダー・プロバイダー・端末間のコンテンツの正規の流通経路をコンテンツに埋めこんで流通させることができるようになる。コンテ

ンツに埋めこまれた透かしを検出することによってコンテンツの正規の流通経路を確認できるようになり、コンテンツの実際の流通経路とコンテンツに埋めこまれた正規の流通経路を比較することにより、コンテンツの流通経路の確かさを確認できるようになる。コンテンツの利用に際しては、確かさのレベルを判定し、その判定結果に応じて利用を制限する機能を端末に設けることにより、例えば音楽コンテンツの再生時に、確かさが低くなるのに応じて多くの雑音を挿入するようにするなど、確かさのレベルに応じた処理ができるようになる。

【 0 0 5 1 】

本発明によれば、コンテンツの流通経路の正当性を判断するための情報をライセンスに代用できるので、高いレベルでのコンテンツ保護ができるようになる。

【 0 0 5 2 】

本発明によれば、コンテンツの流通経路の正当性に応じてコンテンツの利用を制限できるので、コンテンツ・ホルダにとっては、確かな経路でコンテンツを流通させることができるという効果がある。また、コンテンツの利用者も身元の確かなコンテンツを利用できることで安心感が得られる。

【 0 0 5 3 】

いくつかのIDを組み合わせて用いたり、端末側での利用可否の判断を変更することで、保護したいコンテンツのセキュリティレベルに応じた運用ができるという効果もある。

【 0 0 5 4 】

コンテンツの流通経路が不正であると判断した場合は、認証局、もしくは、コンテンツ保証機関に通報する機能によって、不正なコンテンツの流通を発見できるので、ネットポリスがふようであるという効果もある。また、通報しないまでも、不正な流通経路のコンテンツは端末での利用ができなくなるため、不正な流通が拡大しないという効果もある。

【 0 0 5 5 】

【発明の効果】

本発明によれば、プロバイダIDによってデジタルコンテンツを管理するため、コンテンツ・ホルダとコンテンツ利用者の片方又は双方に対しデジタルコンテ

ンツの流通経路を保証するという効果を奏する。

【 0 0 5 6 】

本発明によれば、デジタルコンテンツを不正流通したプロバイダを特定したり、不正流通したデジタルコンテンツの利用を制限するため、デジタルコンテンツの不正流通を抑制できるという効果を奏する。

【図面の簡単な説明】

【図 1】

本発明の一実施例の全体の構成を示した図である。

【図 2】

プロバイダチェックの流れを示した図である。

【図 3】

コンテンツ受信の流れを示した図である。

【図 4】

プロバイダ ID を使用したライセンスチェックの流れを示した図である。

【図 5】

コンテンツ ID の検出の流れを示した図である。

【図 6】

ユーザ ID を使用したライセンスチェックの流れを示した図である。

【図 7】

ユーザ ID とプロバイダ ID とコンテンツ ID を使用したコンテンツ利用の流れを示した図である。

【図 8】

プロバイダ ID を使用したコンテンツの流通経路管理と端末での利用可否の例を表にまとめて示した図である。

【図 9】

コンテンツ ID とプロバイダ ID を使用したコンテンツの流通経路管理と端末での利用可否の例を表にまとめて示した図である。

【図 1 0】

ユーザ ID を使用したコンテンツの流通経路管理と端末での利用可否の例を表に

まとめて示した図である。

【図 1 1】

ユーザ ID とプロバイダ ID を使用したコンテンツの流通経路管理と端末での利用可否の例を表にまとめて示した図である。

【図 1 2】

コンテンツ ID とプロバイダ ID とユーザ ID を使用したコンテンツの流通経路管理と端末での利用可否の例を表にまとめて示した図である。

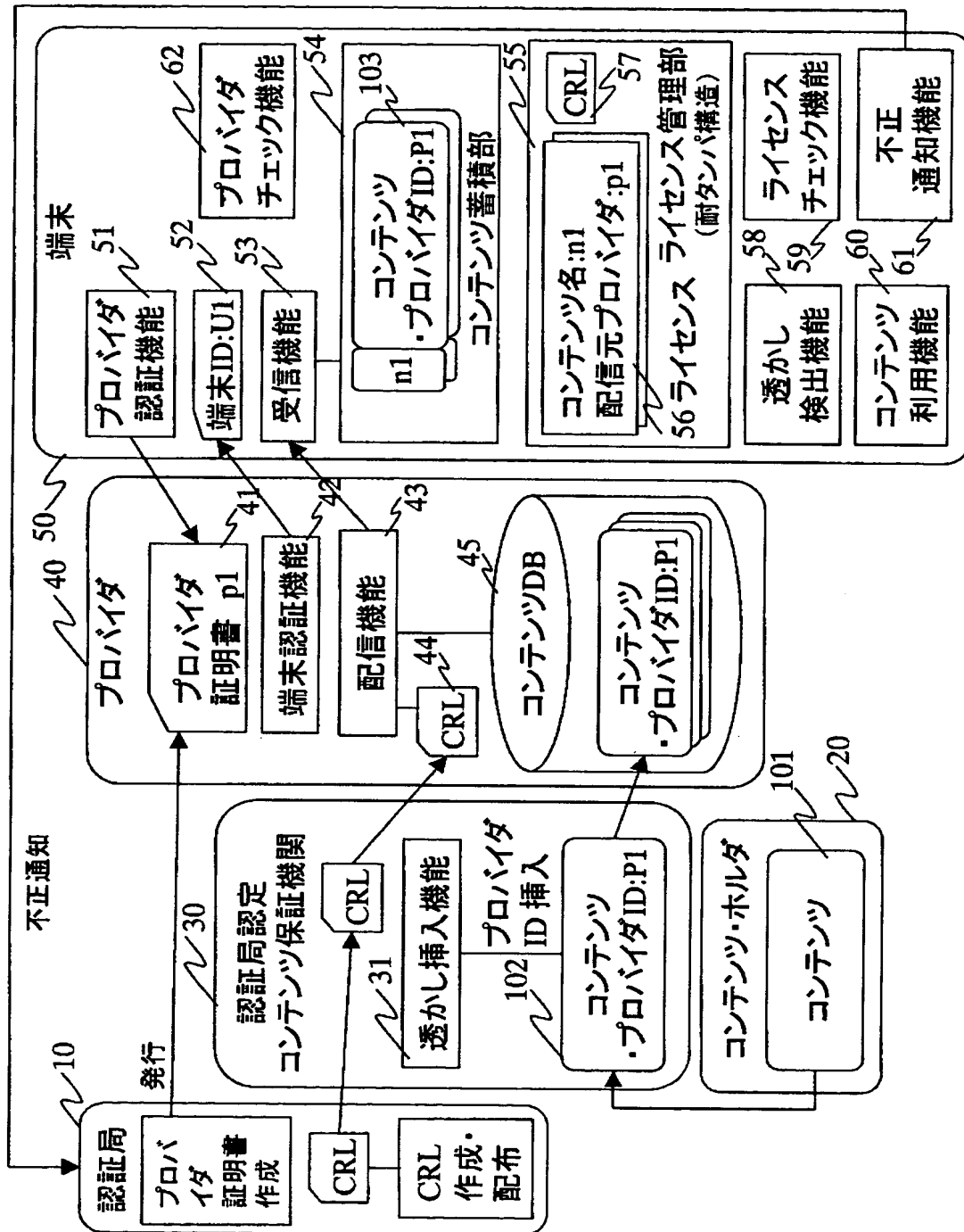
【符号の説明】

1 0 … 認証局、2 0 … コンテンツ・ホルダ、3 0 … コンテンツ保証機関、3 1 … 透かし挿入機能、4 0 … プロバイダ、4 1 … プロバイダ証明書、5 0 … 端末、5 1 … プロバイダ認証機能、5 3 … 受信機能、5 4 … コンテンツ蓄積部、5 5 … ライセンス管理部、5 6 … ライセンス、5 8 … 透かし検出機能、5 9 … ライセンスチェック機能、6 0 … コンテンツ利用機能、6 1 … 不正通知機能、1 0 1, 1 0 2, 1 0 3 … コンテンツ。

【書類名】 図面

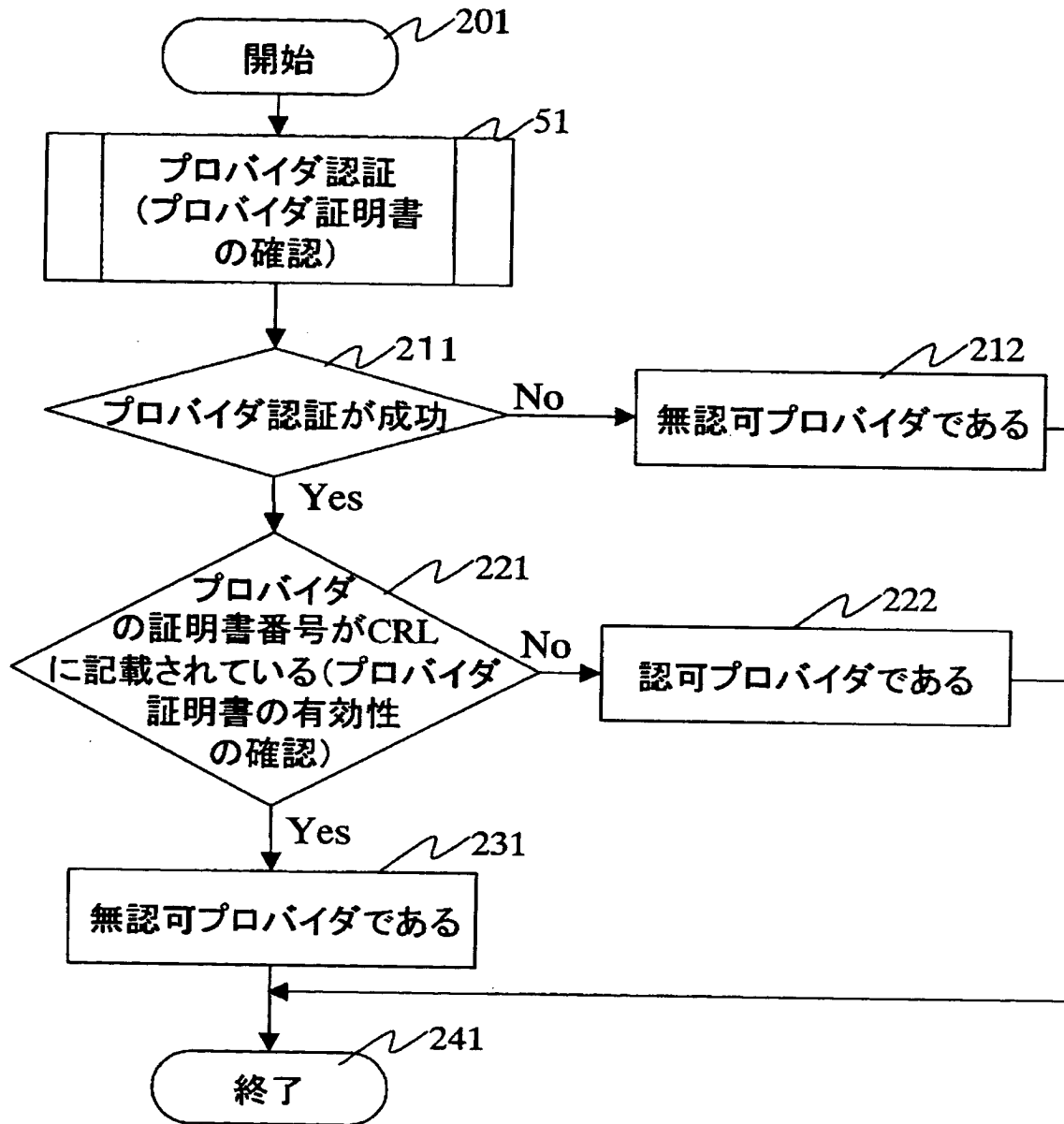
【図 1】

図 1



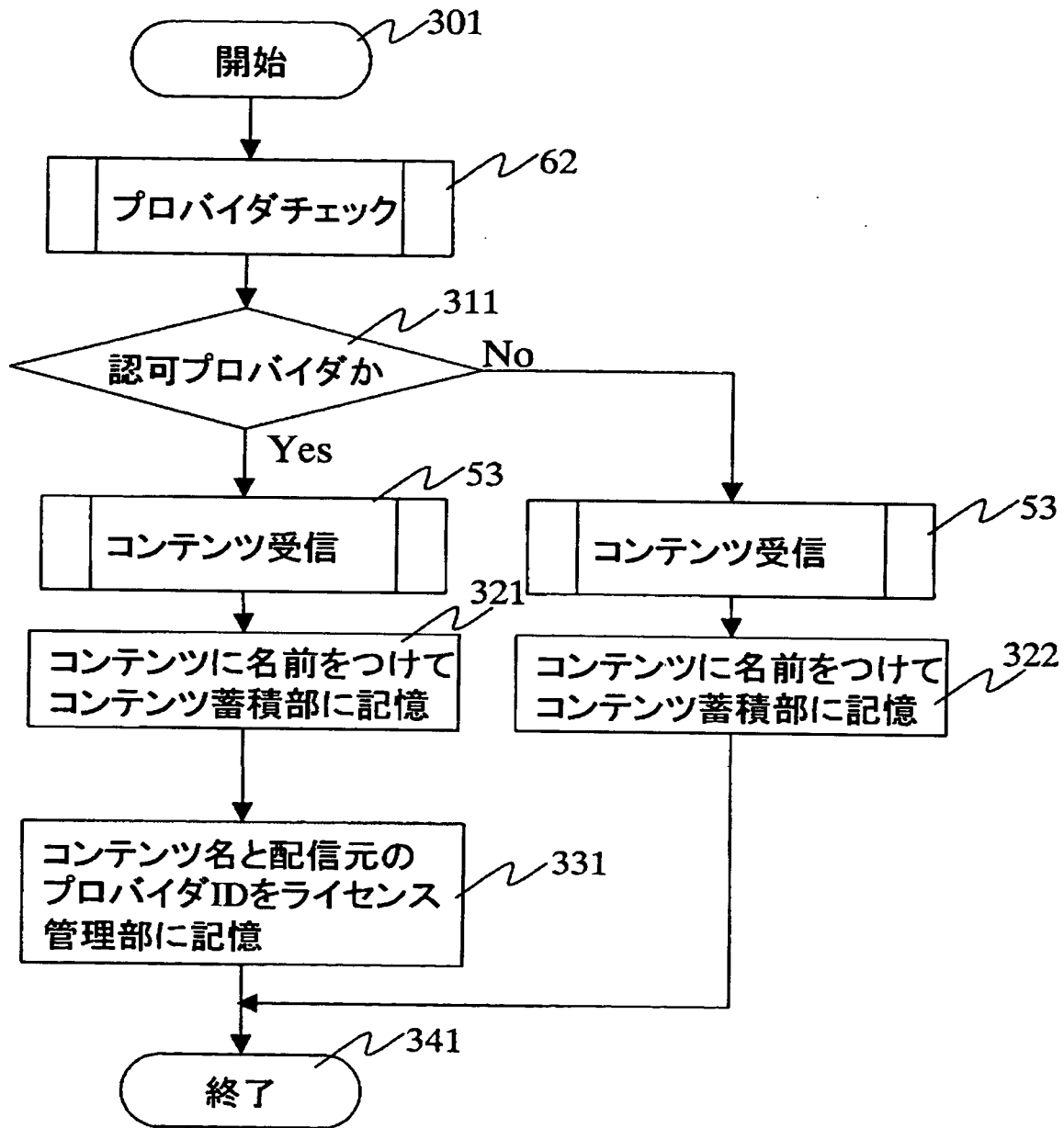
【図 2】

図 2



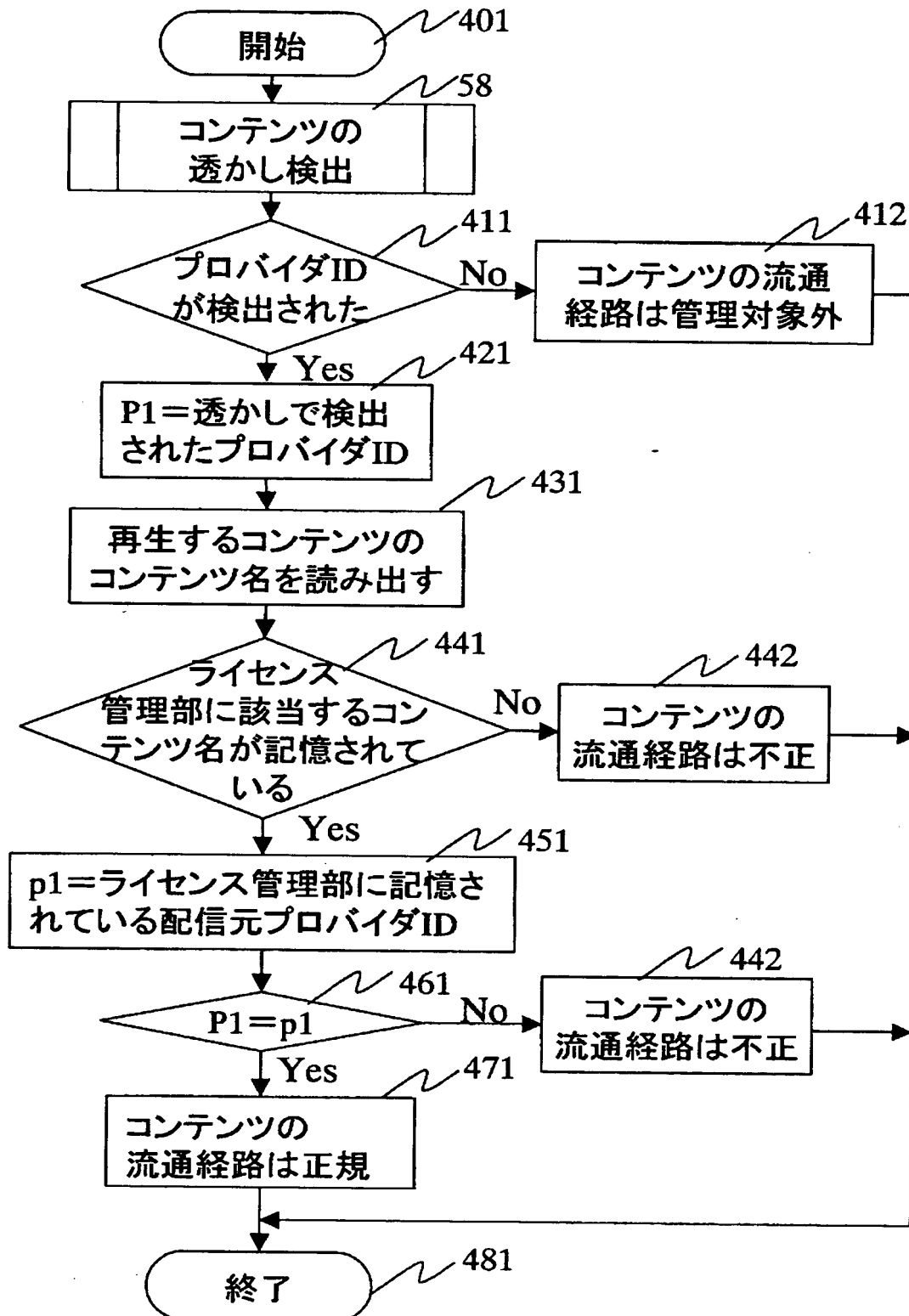
【図 3】

図 3



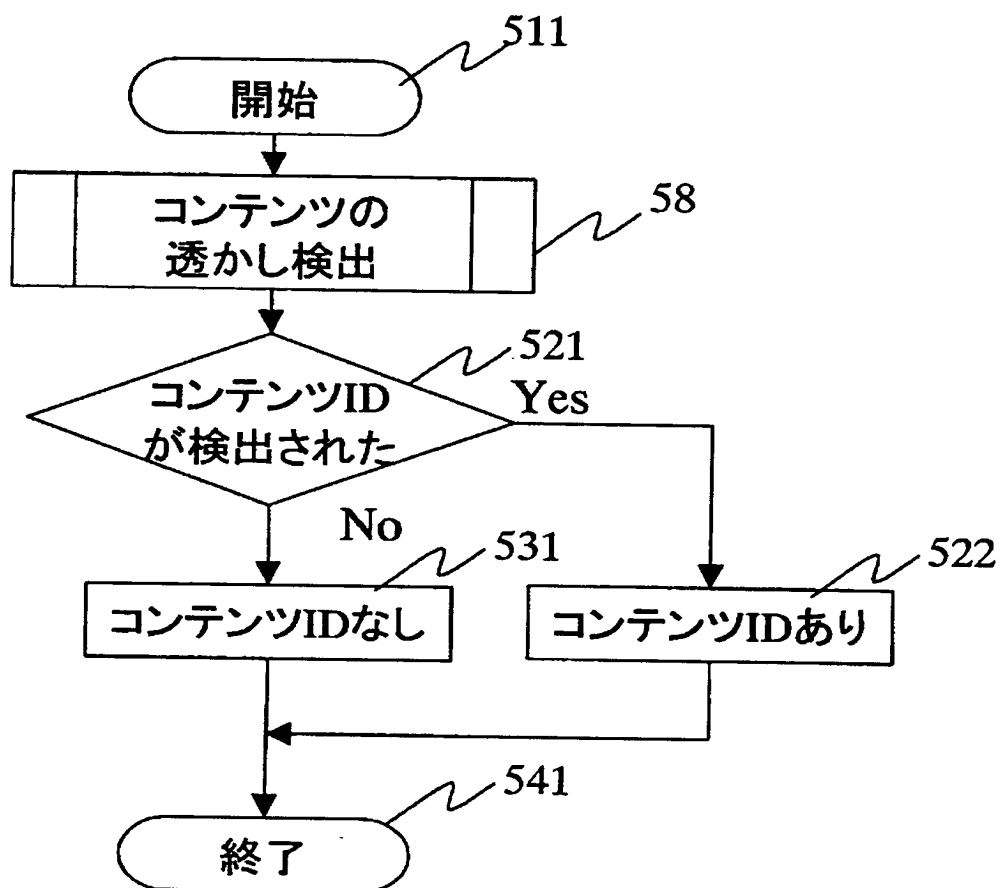
【図 4】

図 4



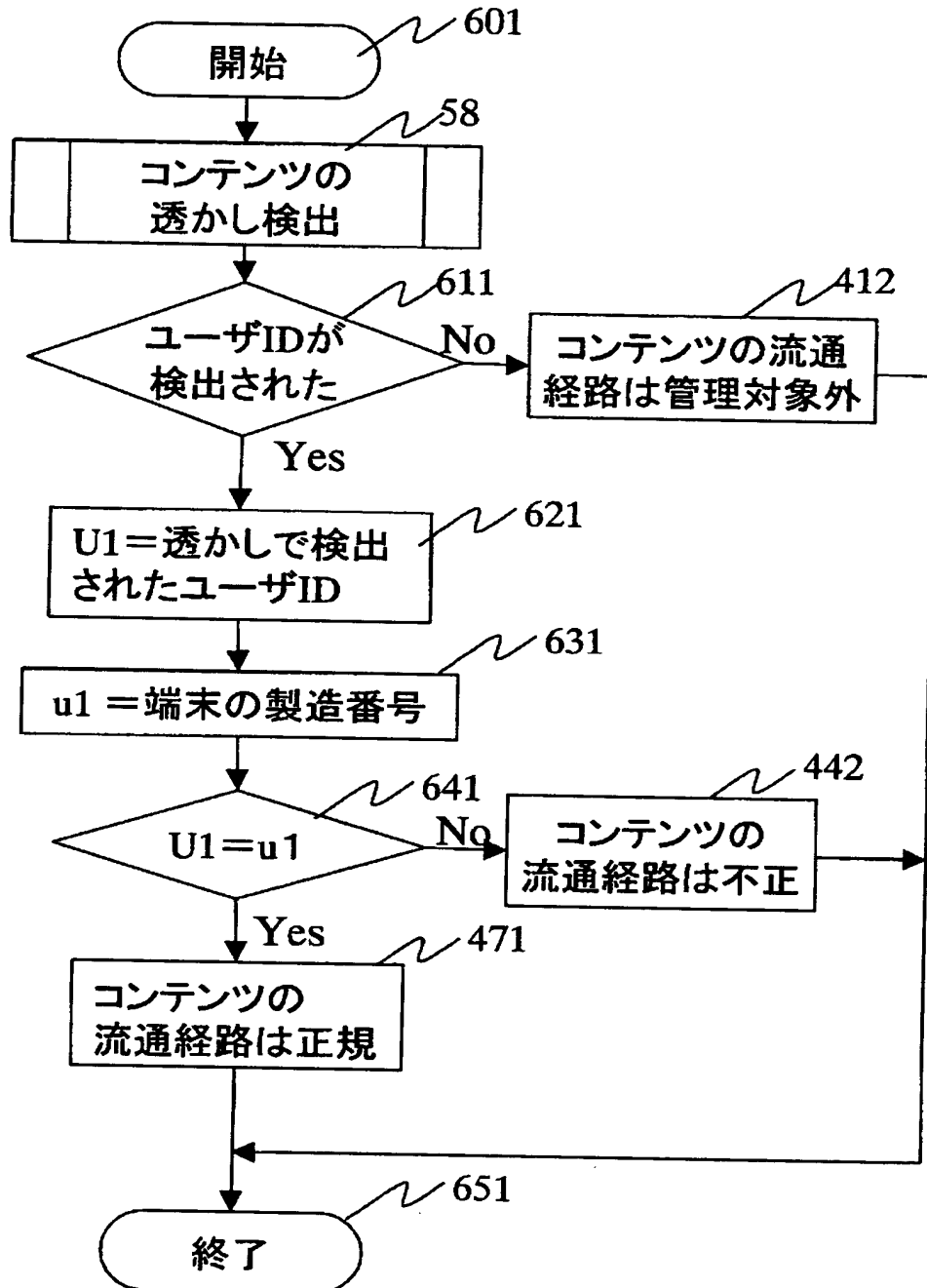
【図5】

図5



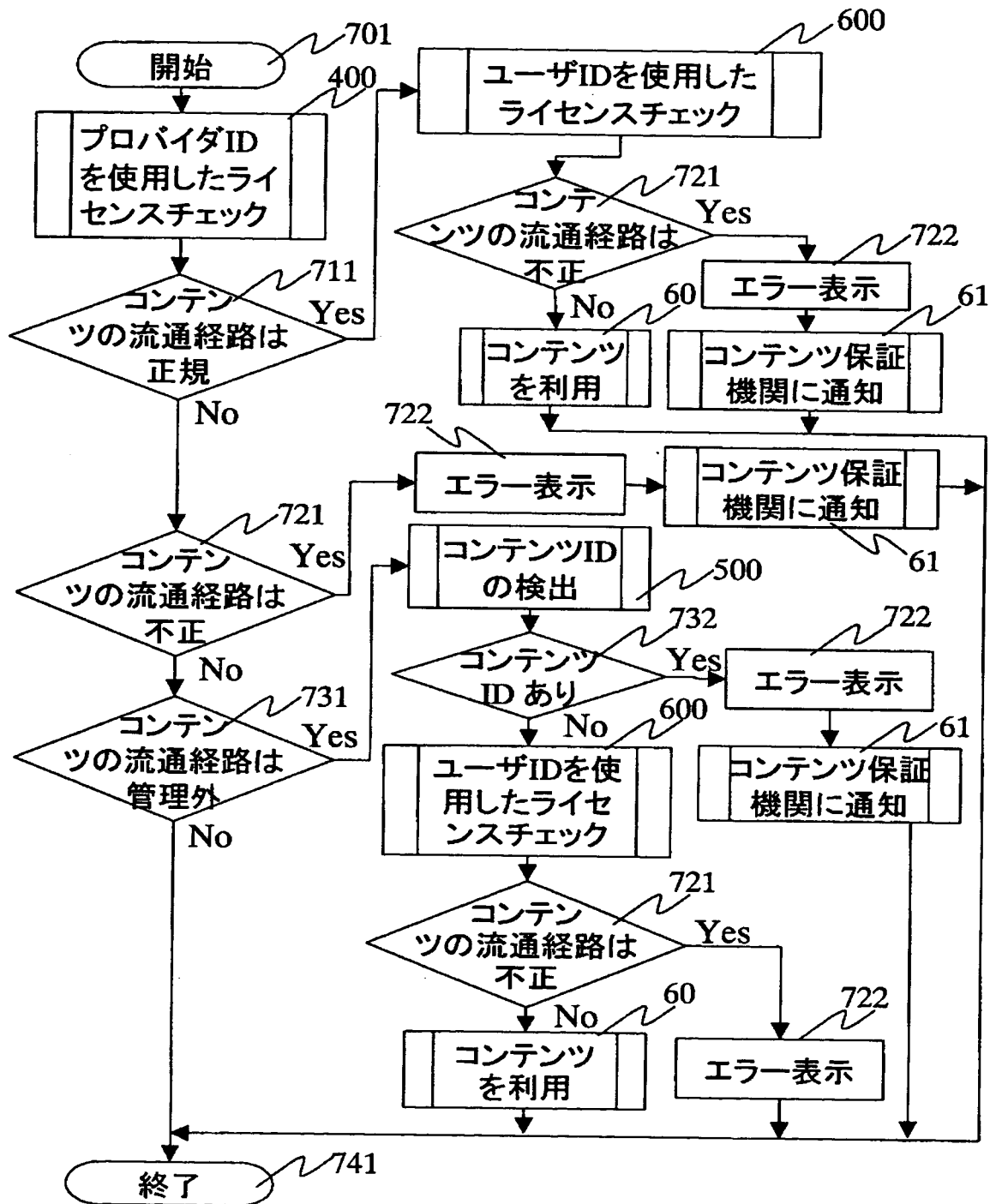
【図 6】

図6



【図 7】

図 7



【図 8】

図 8

プロバイダ IDの透かし	プロバイダ 認証	透かしとプロバイ ダ認証によるプロ バイダIDの一致	コンテンツの プロバイダ流通 経路	コンテン ツの利用
○:有 ×:無	○:認可 ×:無認可	○:一致 ×:不一致 —:比較不能	○:正規 ×:不正 —:管理対象外	○:可 ×:不可
○	○	○	○	○
		×	×	×
○	×	—	×	×
×	○	—	—	○
×	×	—	—	○

【図 9】

図 9

コンテンツ IDの透かし	コンテンツのプロバイ ダ流通経路 (800(図8))	コンテンツの 流通経路	コンテンツの 利用
○:有 ×:無	○:正規 ×:不正 —:管理対象外	○:正規 ×:不正 —:管理対象外	○:可 ×:不可
○	○	○	○
×	○	○	○
○	×	×	×
×	×	×	×
○	—	×	×
×	—	—	○

【図 1 0】

図 10

ユーザIDの 透かし ○:有 ×:無	透かしのユーザID と端末製造番号の 一致 ○:一致 ×:不一致	コンテンツの 端末流通経路 ○:正規 ×:不正 —:管理対象外	コンテンツ の利用 ○:可 ×:不可
○	○	○	○
○	×	×	×
×	—	—	○

【図 1 1】

図 1 1

コンテンツのプ ロバイダ流通経 路(800(図8)) ○:正規 ×:不正 —:管理対象外	コンテンツの端 末流通経路 (900(図9)) ○:正規 ×:不正 —:管理対象外	コンテンツの 流通経路 ○:正規 ×:不正 —:管理対象外	コンテンツの 利用 ○:可 ×:不可
○	○	○	○
○	×	×	×
			保証機関に通知
○	—	プロバイダ:○ 利用端末:—	○
×	○	×	×
			保証機関に通知
×	×	×	×
			保証機関に通知
×	—	×	×
			保証機関に通知
—	○	プロバイダ:— 利用端末:○	○
—	×	プロバイダ:— 利用端末:×	×
—	—	—	○

【図 1 2】

図 12

コンテン ツIDの 透かし ○:有 ×:無	コンテンツのプ ロバイダ流通 経路(900(図9)) ○:正規 ×:不正 —:管理対象外	コンテンツの 端末流通経路 (1000(図10)) ○:正規 ×:不正 —:管理対象外	コンテンツの 流通経路 ○:正規 ×:不正 —:管理対象外	コンテンツの利用 ○:可 ×:不可
○	○	○	○	○
○	○	×	×	× 保証機関に通知
○	○	—	プロバイダ:○ 利用端末:—	○
×	○	○	○	○
×	○	×	×	× 保証機関に通知
×	○	—	プロバイダ:○ 利用端末:—	○
○	×	○	×	× 保証機関に通知
○	×	×	×	× 保証機関に通知
○	×	—	×	× 保証機関に通知
×	×	○	×	× 保証機関に通知
×	×	×	×	× 保証機関に通知
×	×	—	×	× 保証機関に通知
○	—	○	×	× 保証機関に通知
○	—	×	×	× 保証機関に通知
○	—	—	×	× 保証機関に通知
×	—	○	プロバイダ:— 利用端末:○	○
×	—	×	×	×
×	—	—	—	○

【書類名】 要約書

【要約】

【課題】

本発明は、コンテンツ・ホルダとコンテンツ利用者の片方又は双方に対しデジタルコンテンツの流通経路を保証し、又は、デジタルコンテンツの不正流通を抑制することを課題とする。

【解決手段】

プロバイダ 4 0 が配信するプロバイダ 4 0 のプロバイダ I D を電子透かしを用いて埋め込む。端末 5 0 は、プロバイダ 4 0 の証明書 4 1 を確認し、証明書 4 1 に記載されているプロバイダ I D とコンテンツ I D の組 5 6 をライセンス管理部 5 5 に記憶する。端末 5 0 では、コンテンツの利用時にはプロバイダ I D の透かしを検出し、耐タンバ領域に記憶されたプロバイダ I D と透かしに埋め込まれたプロバイダ I D とが一致しているかどうかによって、コンテンツの利用の可否を決定する。

【選択図】 図 1

特 2002-321962

認定・付加情報

特許出願の番号	特願 2002-321962
受付番号	50201672076
書類名	特許願
担当官	第七担当上席 0096
作成日	平成14年11月 7日

<認定情報・付加情報>

【提出日】 平成14年11月 6日

次頁無

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所